


TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

(chapitre II du Traité de coopération en matière de brevets)

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE À DONNER voir formulaire PCT/PEAA416	
Demande internationale No. PCT/IB2004/051130	Date du dépôt international (<i>jour/mois/année</i>) 06.07.2004	Date de priorité (<i>jour/mois/année</i>) 14.07.2003
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L29/06		
Déposant NAGRAVISION SA		
<p>1. Le présent rapport est le rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international en vertu de l'article 35 et transmis au déposant conformément à l'article 36.</p> <p>2. Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.</p> <p>3. Ce rapport est accompagné d'ANNEXES, qui comprennent :</p> <p>a. <input checked="" type="checkbox"/> un total de (<i>envoyées au déposant et au Bureau international</i>) 3 feuilles, définies comme suit :</p> <p><input checked="" type="checkbox"/> les feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou des feuilles contenant des rectifications autorisées par la présente administration (voir la règle 70.16 et l'instruction administrative 607).</p> <p><input type="checkbox"/> des feuilles qui remplacent des feuilles précédentes, mais dont la présente administration considère qu'elles contiennent une modification qui va au-delà de l'exposé de l'invention qui figure dans la demande internationale telle qu'elle a été déposée, comme il est indiqué au point 4 du cadre n° I et dans le cadre supplémentaire.</p> <p>b. <input type="checkbox"/> (<i>envoyées au Bureau international seulement</i>) un total de (préciser le type et le nombre de support(s) électronique(s)) , qui contiennent un listage de la ou des séquences ou un ou des tableaux y relatifs, déposés sous forme déchiffrable par ordinateur seulement, comme il est indiqué dans le cadre supplémentaire relatif au listage de la ou des séquences (voir l'instruction administrative 802).</p>		
<p>4. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :</p> <p><input checked="" type="checkbox"/> Cadre n° I Base de l'opinion</p> <p><input type="checkbox"/> Cadre n° II Priorité</p> <p><input type="checkbox"/> Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle</p> <p><input type="checkbox"/> Cadre n° IV Absence d'unité de l'invention</p> <p><input checked="" type="checkbox"/> Cadre n° V Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration</p> <p><input type="checkbox"/> Cadre n° VI Certains documents cités</p> <p><input type="checkbox"/> Cadre n° VII Irrégularités dans la demande internationale</p> <p><input type="checkbox"/> Cadre n° VIII Observations relatives à la demande internationale</p>		
Date de présentation de la demande d'examen préliminaire internationale 28.04.2005	Date d'achèvement du présent rapport 01.08.2005	
Nom et adresse postale de l'administration chargée de l'examen préliminaire international  Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Veen, G N° de téléphone +31 70 340-3811	



**RAPPORT PRÉLIMINAIRE INTERNATIONAL
SUR LA BREVETABILITÉ**

Demande internationale n°
PCT/IB2004/051130

Cadre n° V Déclaration motivée selon l'article 35.2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

- | | | | |
|--|------|----------------|------|
| 1. Déclaration | | | |
| Nouveauté | Oui: | Revendications | 1-11 |
| | Non: | Revendications | |
| Activité inventive | Oui: | Revendications | 1-11 |
| | Non: | Revendications | |
| Possibilité d'application industrielle | Oui: | Revendications | 1-11 |
| | Non: | Revendications | |

2. Citations et explications (règle 70.7) :

voir feuille séparée

- 1 Dans la présente notification, il est fait référence au document suivant:

D1: WO 01/67705 A (DOHERTY BRIAN JOHN O ;HERBERT STREET
TECHNOLOGIES LT (IE); TARAROU) 13 septembre 2001 (2001-09-13)

2 **Concernant le point V**

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

2.1 **REVENDEICATION 1**

L'état de la technique le plus proche, représenté par D1, divulgue un procédé de transfert sécurisé de données d'un ordinateur à un autre, à travers l'Internet, par l'intermédiaire d'un serveur. Le transfert est effectué sur l'écran d'un ordinateur, en glissant les données à transférer d'une fenêtre transmetteur à une fenêtre récepteur. L'action de glisser les données d'une fenêtre à une autre a pour effet de restituer et rechiffrer les données avec les clés correspondantes.

La méthode de la revendication 1 diffère de D1 en ce que la restitution et le rechiffrement sont effectués par un dispositif connecté à un réseau local sécurisé, de manière que, après le rechiffrement, un autre dispositif ("dispositif de restitution") autorisé, connecté au même réseau, peut déchiffrer les données.

Le problème résolu par ces aspects peut être défini comme "comment distribuer des données sur un réseau local de façon qu'ils ne puissent être accessibles qu'à un autre dispositif autorisé, connecté au même réseau".

Comme aucun des documents disponible révèle ou indique un tel système, la revendication 1 satisfait aux exigences des Articles 33(2) et 33(3) PCT.

2.2 **REVENDEICATIONS 2-13**

Les revendications 2-13 sont dépendantes de la revendication 1, alors elles satisfont aussi aux exigences du PCT concernant nouveauté et activité inventive.

REVENDECATIONS

1. Méthode de création et d'administration d'un réseau local, ce réseau comprenant au moins un **dispositif de diffusion et de rechliffement (MD)** d'un **flux de données chliffées** et un **dispositif de restitution (DV)** de tout ou partie desdites données chliffées, ces dispositifs comprenant des modules de sécurité (CC, TC, MC), cette méthode comprenant les étapes suivantes initiales :

- connexion d'un module de sécurité (MC) dit maître dans un dispositif (MD) de diffusion et de rechliffement ou dans un dispositif de restitution (DV) connecté au réseau local,
- établissement d'une clé de réseau (NK) par ledit module de sécurité maître (MC),
- transmission sécurisée de cette clé de réseau (NK) à un ou des modules de sécurité dits utilisateur (TC),

et lors de la réception d'un flux de données chliffées par un point d'accès du réseau :

- réception par un ledit dispositif de diffusion et de rechliffement (MD) du flux de données chliffées;
- vérification par le module de sécurité (CC) lié audit dispositif de diffusion et de rechliffement (MD) de l'existence de droit d'accès audit flux de données chliffées;
- en cas d'existence des droits, déchiffrement des données chliffées grâce aux informations fournies par le module de sécurité (CC) associé à ce dispositif de diffusion et de rechliffement (MD);
- rechliffement des données par ledit dispositif de diffusion et de rechliffement (MD) par une clé locale,
- transmission des données rechliffées par ladite clé locale au dispositif de restitution (DV),
- déchiffrement par ledit dispositif de restitution (DV) grâce au module de sécurité utilisateur (TC) qui lui est associé disposant de moyens pour retrouver la clé locale.

- 2. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que lesdites données comportent une partie utile chiffrée d'une part et une partie de gestion en charge du contrôle du déchiffrement de cette partie utile chiffrée d'autre part, et en ce que les étapes de déchiffrement et de rechiffrement des données sont appliquées à la partie utile.**
- 3. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que lesdites données comportent une partie utile chiffrée d'une part et une partie de gestion en charge du contrôle du déchiffrement de cette partie utile chiffrée d'autre part, et en ce que les étapes de déchiffrement et de rechiffrement des données sont appliquées à la partie de gestion.**
- 4. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que la clé locale est une clé de session générée aléatoirement et chiffrée par la clé de réseau.**
- 5. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que la clé locale est la clé de réseau.**
- 6. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que l'établissement de la clé de réseau est obtenue par génération pseudo-aléatoire d'une clé lors de l'initialisation du réseau local.**
- 7. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que l'établissement de la clé de réseau est effectuée lors d'une étape d'initialisation du module maître.**
- 8. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que le module maître est localisé dans un module de sécurité amovible.**
- 9. Méthode de création et d'administration d'un réseau local selon la revendication 7, caractérisée en ce que ce module de sécurité amovible**

comprend un module utilisateur faisant partie du réseau administré par le module maître.

10. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que les modules de sécurité utilisateur sont sous forme d'un circuit électronique monté lors de la fabrication du dispositif de restitution.

11. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que le module de sécurité utilisateur est sous forme d'un module de sécurité amovible.

12. Méthode de création et d'administration d'un réseau local selon la revendication 1, caractérisée en ce que le dispositif de diffusion et de rechiffrement comprend un module de sécurité dit module convertisseur, ce module recevant et conservant un identifiant du module maître ayant créé le réseau pour lequel le module convertisseur rechiffre des données.

13. Méthode de création et d'administration d'un réseau local selon la revendication 10, caractérisée en ce que cet identifiant du module maître est transmis à un centre de gestion lors d'une phase de connexion avec ledit centre de gestion.